

REMARKS*Claim Amendments*

Applicants respectfully request entry of the foregoing claim amendments, which are discussed further below. No new matter is introduced.

The amendments are permissible in response to the Final Rejection because they are made to place the claims in better condition for appeal. *See* 37 CFR 1.116(b)(2). Applicants also note that the finality of the Office Action is improper, since a new reference (Mital) was cited.

Rejections under 35 U.S.C. § 103

Claims 1-2, 7-8, 16-19, 20-21, 25-26, and 34-37 are rejected under 35 U.S.C. § 103 due to U.S. Pat. No. 6,081,793 of Challener *et al.* (here, “Challener *et al.*”) in view of U.S. Pat. No. 5,903,652 of Mital (here, “Mital”). Also, dependent claims 3-4, 9-12, 22-23, and 27-30 are rejected over Challener *et al.* in view of Schneier (cited in previous Office Action); dependent claims 13-15, 31-33, and 38 are rejected over Challener *et al.* in view of Ansell *et al.* (cited in previous Office Action); and dependent claim 39 is rejected over Challener *et al.* in view of Coss *et al.* (EP 0 909 074 A1).

As discussed below, Applicants respectfully traverse these rejections and request reconsideration and allowance of all claims.

Independent Claims 1 and 20: the Secret Sharing Feature

An important feature of independent claims 1 and 20 is neither disclosed nor suggested by Challener *et al.* or Mital: the use of secret sharing techniques to control access to an anonymous mapping that allows research data to be rendered anonymous. To further clarify this distinction, Applicants have amended independent apparatus claim 1 to state that the secret sharing module includes the following features: “a secret sharing module stored on a computer-readable medium for performing secret sharing to control keyholder access to the mapping module such that a predetermined number of keyholders greater than one is required to compromise access to the mapping module.” This claim amendment finds support at Page 10,

lines 4-5 of the Specification as originally filed, among other places. A similar amendment is made to independent method claim 20.

This claim amendment makes clear what is meant by the secret sharing module: the secret sharing module controls access to the mapping module such that a predetermined number of keyholders greater than one is required to compromise access to the mapping. For example, as discussed in the Application at Page 10, line 1, through Page 12, line 6, multiple keyholders M may be required to enter their passwords at system startup in order to generate the data encryption key K used by the mapping module. Certain procedures may be used to allow the retirement and replacement of keyholders, and to restart the system and regenerate the encryption key K.

By contrast, there is no disclosure or suggestion of any secret sharing techniques in Challener *et al.*, which relates entirely to the use of conventional public/private key encryption techniques. The claimed use of secret sharing is not the same as conventional public/private key encryption because the claimed secret sharing requires multiple keyholders to compromise access to the mapping.

By contrast, the portions of Challener *et al.* cited in the Office Action do not involve requiring multiple keyholders to access an anonymous mapping. In the "Response to Arguments" section of the Office Action, it is stated that Challener *et al.* discloses the use of a secret sharing module, as follows: "[T]he user PC performs secret sharing... by encrypting the ballot and only allowing access to the authentication server (mapping module) [to those who possess] the key to decrypt the encrypted information."

However, the interaction of the voter with the authentication server in Challener *et al.* does not involve the claimed control of access to an anonymous mapping module using secret sharing by requiring multiple keyholders. Instead, as described at Col. 3, lines 10-36, each voter's public key and private key is stored on an authentication server 225, and optionally, in an escrow service 221. There is no disclosure or suggestion that access to the authentication server 225 or escrow service 221 is maintained by secret sharing that requires the presence of multiple keyholders.

Furthermore, neither the authentication server 225 nor the escrow service 221 functions as a mapping module for performing an anonymous mapping. As described at Col. 7, line 40

through Col. 8, line 8, the authentication server 225 merely authenticates the user and provides the user with a ballot ID; it does not perform any anonymous mapping. The escrow service 221 likewise does not perform any anonymous mapping, instead simply storing a public/private key library (see Col. 3, lines 29-36).

The cited use of the authentication server 225 in Challener *et al.* therefore does not disclose or suggest the use of a secret sharing module to require multiple keyholders to access an anonymous mapping module of the present invention.

Similarly, Applicants respectfully traverse the statement in the Office Action that the claimed secret sharing module is disclosed in items 379, 391, and 439 of Fig. 7 of Challener *et al.* Instead, item 379 relates to a voter's request for a ballot, which uses a conventional public key; item 391 relates to the authentication server 225 sending an encrypted ballot to the voter, again using conventional public keys; and item 439 relates to a results server 229 tabulating the results of an election. None of these items involve requiring multiple keyholders to allow access to an anonymous mapping module.

Challener *et al.* therefore does not disclose or suggest the claimed use of a secret sharing module to require multiple keyholders to access an anonymous mapping module, which is recited in both independent claims 1 and 20.

Likewise, there is no disclosure or suggestion of any secret sharing techniques in Mital, which relates entirely to the use of conventional public/private key encryption techniques. The portions of Mital cited in the Office Action do not involve requiring multiple keyholders to access an anonymous mapping module. The "Response to Arguments" section of the Office Action appears to maintain that the Secured Technology Module 304 (Fig. 3) of the consumer computer 100 (Fig. 1) of Mital corresponds to the claimed secret sharing module; that the Electronic Commerce Service 104 (Fig. 1) corresponds to the claimed mapping module; and that the use of an encrypted Goods and Services Order/Payment Instruction packet sent from the consumer 100 to the Electronic Commerce Service 104 is the claimed use of a secret sharing module. However, Mital's use of an encrypted packet sent from the consumer 100 to the Electronic Commerce Service 104 does not involve the claimed use of a secret sharing module to require multiple keyholders in order to access an anonymous mapping module. Instead, the consumer 100 is merely sending a standard public/private key encrypted packet to the Electronic

Commerce Service 104, and is not controlling access to the Electronic Commerce Service 104. The Electronic Commerce Service 104 does have its own Online Network Private Key 408 of Fig. 4, but this is not provided to consumers. Nor can the consumer's own use of private key encryption of its payment instructions be said to involve the use of multiple keyholders to control access to a mapping module, since the merchant uses only one key to access the goods and services order, the acquirer uses only one key to access its payment instructions, and, in doing so, neither the merchant nor the acquirer is accessing an anonymous mapping module.

Thus, neither Challenger *et al.* nor Mital discloses or suggests the claimed use of a secret sharing module to require multiple keyholders to access an anonymous mapping module, which is recited in both independent claims 1 and 20. Because neither reference discloses or suggests this feature separately, their combination also does not disclose or suggest this feature.

Independent Claims 1 and 20: Mapping Module Accessing Both Identifiers and Working Data

Another feature of independent claims 1 and 20 also serves to distinguish those claims over Challenger *et al.* and Mital. The Office Action concedes (in the last paragraph of Page 4) that Challenger *et al.* does not disclose or suggest a feature of independent claims 1 and 20, "... wherein the mapping module is capable of accessing both the identifier portion and the research data portion of the working data." The Office Action states that Mital discloses use of such a feature at Col. 27, lines 54-61.

However, this passage of Mital does not disclose or suggest the claimed feature of an anonymous mapping module capable of accessing both the identifier portion and the research data portion of working data. Instead, this passage of Mital relates to the consumer computer 100 using encryption to encrypt the payment information that is ultimately decrypted by the acquirer computer 112 (e.g. a credit company). It does not relate to an anonymous mapping module capable of accessing both an identifier portion and a research data portion of working data, because the consumer computer 100 cannot be said to be the claimed anonymous mapping module. The consumer computer 100 is, in fact, sending out a Goods and Services Order and Payment Instructions that include the consumer's personal information, and which is therefore not anonymous. Mital's technique is intended to allow electronic commerce in which the merchant knows the consumer's identity in order to be able to ship them their goods. Therefore,

Mital does not use an anonymous mapping to obscure the consumer's identity from the merchant. The consumer computer 100 therefore cannot be said to be the claimed anonymous mapping module, taking the merchant as the recipient.

Further, it could not be maintained that the consumer computer 100 is the claimed mapping module, with the electronic commerce service 104 taken as the recipient, because there is no disclosure or suggestion of requiring multiple keyholders to control access to the encryption used by the consumer computer, as required of the claimed mapping module.

Therefore, neither Challener *et al.* nor Mital discloses or suggests the claimed use of an anonymous mapping module that is capable of accessing both the identifier portion and the research data portion of the working data, which is recited in both independent claims 1 and 20. Because neither reference discloses or suggests this feature separately, their combination also does not disclose or suggest this feature.

Independent Claims 1 and 20: Communication Module Transmitting both an Anonymously Mapped Identifier and Unmapped Research Data

A further feature of independent claims 1 and 20 further serves to distinguish those claims over Challener *et al.* and Mital: "...wherein the communication module is capable of transmitting both the anonymously mapped identifier portion and the unmapped research data portion of the working data to the receiver."

The Office Action asserts, without support, that Challener *et al.* discloses this feature. Further, the Office states that Mital discloses this feature at Col. 7, line 65 through Col. 8, line 14.

Such a communication module is not disclosed or suggested by Challener *et al.* because Challener *et al.* does not involve transmitting both an anonymously mapped identifier portion and a working data portion of research data to the results server 229. Instead, journal server 227 receives both a completed ballot and a voter ID; and sends only the completed ballot on to a results server 229. Challener *et al.* does not disclose or suggest that the journal server 227 would map the voter ID using an anonymous mapping and send it on to the results server 229 along with the completed ballot. Therefore, Challener *et al.* does not disclose or suggest a

communication module capable of transmitting both an anonymously mapped identifier and an unmapped research data portion to a receiver.

Mital likewise does not disclose or suggest the claimed feature of a communication module capable of transmitting both the anonymously mapped and unmapped portions. At Col. 7, line 65 through Col. 8, line 14, Mital describes a consumer computer 100 sending a secure purchase order message 102 to an electronic commerce service 104. The secure purchase order message 102 (shown later in Fig. 7) includes a goods and services order (Fig. 8B), a payment instruction (Fig. 8A), and audit information (Fig. 9). The goods and services order is only decryptable by a merchant computer 108 (Fig. 1); the payment instruction is only decryptable by an acquirer computer 112; and the audit information is only decryptable by an electronic commerce service 104.

However, Mital's use of a consumer computer 100 sending a secure purchase order message 102 does not disclose or suggest the claimed communication module capable of transmitting both an anonymously mapped and unmapped portion of working data. In particular, the secure purchase order message 102 does not include the claimed anonymously mapped data because the Goods and Services Order includes the consumer's personal information. This information is intended to be decrypted by the recipient, the merchant 108. Mital's technique is intended to allow electronic commerce in which the merchant knows the consumer's identity in order to be able to ship them their goods. Therefore, Mital does not use an anonymous mapping to obscure the consumer's identity from the merchant. The consumer computer 100 therefore cannot be said to be the claimed communication module, taking the merchant as the recipient.

Further, if it were to be maintained that the consumer computer 100 was the claimed communication module, with the electronic commerce service 104 taken as the recipient, that would imply that the consumer computer 100 was also the claimed mapping module, since the claim language involves the consumer computer 100 sending data that has already been anonymously mapped. However, the consumer computer 100 is not the claimed mapping module, because there is no disclosure or suggestion of requiring multiple keyholders to control access to the encryption used by the consumer computer, as required of the claimed mapping module.

Thus, Mital's use of the consumer computer 100 does not disclose or suggest the claimed communication module capable of transmitting both an anonymously mapped and unmapped portion of working data.

Therefore, neither Challener *et al.* nor Mital discloses or suggests the claimed use of a communication module that is capable of transmitting both the anonymously mapped identifier portion and the unmapped research data portion of the working data to the receiver, which is recited in both independent claims 1 and 20. Because neither reference discloses or suggests this feature separately, their combination also does not disclose or suggest this feature.

Construction of the Term "Working Data Identifier Set Domain"

Applicants must respectfully traverse the statements in the Office Action at Page 3, first paragraph, and Page 4, second and third paragraphs, regarding the definition of "working data identifier set domain."

Applicants submit that the definition of this claim term should be interpreted by standard claim interpretation techniques rather than being interpreted according to the language given in the Office Action.

"To ascertain the meaning of claims, we consider three sources: The claims, the specification, and the prosecution history." *Markman v. Westview Instruments, Inc.*, 52 F.3d 967, 979 (Fed. Cir. 1995) (*en banc*), *aff'd*, 517 U.S. 370 (1996) (citation omitted). Of these three sources, "[f]irst, we look to the words of the claims themselves, both asserted and nonasserted, to define the scope of the patented invention." *Vitronics Corp. v. Conceptronic, Inc.*, 90 F.3d 1576, 1582 (Fed. Cir. 1996). Second, the claims must be read in view of the specification, of which they are a part. *Phillips v. AWH Corp.*, 415 F.3d 1303, 1313 (Fed. Cir. 2005) *cert. den.*, 164 L.Ed.2d 49 (U.S., 2006). The Federal Circuit recently affirmed that the specification is "always highly relevant to the claim construction analysis," and is usually "the single best guide to the meaning of a disputed claim term." *Id.*

Taking these principles as a guide, we first look at the words of the claim term themselves: "working data identifier set domain." Those words require: 1) a domain, which is 2) associated with an identifier set, which is 3) associated with working data. Thus, the words themselves involve domains that are differentiated from one another by the characteristics of the

identifier sets associated with the underlying working data. As a concrete example from the Application, the working data in one domain, the Data Collector domain, may have a certain type of identifier set: namely, personal identifiers that are unchanged from their original form, revealing the identities or other personal information of persons associated with the underlying data. By contrast, the working data in another domain, the Data Analyzer domain, may have a different type of identifier set: namely, personal identifiers that have been anonymously mapped by an anonymous mapping so that they no longer reveal the identities or other personal information of the persons associated with the working data.

Next, having looked at the words of the claim term “working data identifier set domain” themselves, Applicants note that the concept of the working data identifier set domain is discussed in the present Application at page 12, line 25 through page 13, line 3, among other places. Contrary to the statement in the Office Action at Page 3, first paragraph, Applicants have not, and do not, maintain that there is an explicit “definition” of the claim term at that location. Rather, that location, among others, serves as a guide to interpreting the claim term in accordance with the standard claim interpretation principles given above.

In particular, the Application at Page 12, line 25 through Page 13, line 3 makes reference to Figure 5, in which secret mapping is used between multiple domains. At Page 12, lines 26-28, it is stated: “For instance, two domains might be the set of identifiers in two different laboratories working with anonymous data and the third domain the social-security identifiers.” Thus, this passage illustrates that different domains may be associated with different identifier sets: for example, a first laboratory in one domain might identify people by one set of anonymous identifiers; a second laboratory in a second domain might identify people by a second set of anonymous identifiers; and a third domain might identify people by their actual social-security identifiers. The words of the passage at Page 12, line 25 through Page 13, line 3 are illustrated further by Figure 5, in which domains D_i 501, D_j 502, and D_k 503 are related by one-to-one mapping relations, DM_{ij} 504 and DM_{jk} 505.

Thus, the meaning of the claim term “working data identifier set domain” is further illustrated by this passage and the associated figure, which disclose the use of 1) a domain, which is 2) associated with an identifier set, which is 3) associated with working data.

Turning to the definition of this claim term given in the Office Action, it is stated at Page 4, second paragraph, that the definition should be “data that devices process that are divided into sets.” Such a definition ignores both the words of the claim term themselves and the specification, which are two of the most important sources of claim construction. In particular, the definition given in the Office Action ignores the word “domain” and the phrase “identifier set,” and essentially truncates the words to be only “working data sets.” Such a definition therefore impermissibly ignores words in the claim, and also the illustrative use of those words in the specification.

Thus, Applicants respectfully submit that the claim term “working data identifier set domain” should not be construed as given in the Office Action, but rather, based on standard claim interpretation techniques, should involve 1) a domain; which is 2) associated with an identifier set; which is 3) associated with working data.

Using such a construction, Applicants submit that the claims are not disclosed or suggested by the cited art for the reasons given above, which are, in any event, valid reasons independent of the exact construction of this claim term.

Summation and Dependent Claims

For the foregoing reasons, Applicants therefore submit that Challener *et al.* in view of Mital does not disclose or suggest the inventions of independent claims 1 and 20, and request reconsideration and allowance of those claims. Because dependent claims 2, 7-8, 16-19, 21, 25-26, and 34-37 incorporate the features of base claims 1 and 20, they are also allowable for the foregoing reasons.

Also, neither Schneier, nor Ansell *et al.*, nor Coss *et al.*, which are applied to several of the dependent claims, discloses or suggests the foregoing features. In particular, those references do not disclose or suggest (i) the use of secret sharing to control keyholder access to Applicants’ claimed mapping module by requiring multiple keyholders; nor (ii) a mapping module such as that claimed by Applicants that is capable of accessing both the identifier portion and the research data portion of the working data; nor (iii) a communication module capable of transmitting both an anonymously mapped identifier and an unmapped research data portion to a receiver; nor the preceding three features in combination. Applicants therefore submit that

dependent claims 3-4, 9-15, 22-23, 27-33, 38, and 39 are also allowable for the foregoing reasons.

Claims 40 and 41


Claims 40 and 41 were not addressed in the Office Action, although they were noted as being currently pending in the first paragraph of page 2 of the Office Action and were listed as rejected in the check-boxes on page 1 of the Office Action. Therefore, for the sake of clarity, Applicants submit that Claims 40 and 41 are also allowable for the reasons given above for their respective base claims 1 and 20, and request reconsideration and allowance of those claims.

CONCLUSION

In view of the above amendments and remarks, it is believed that all claims are in condition for allowance, and it is respectfully requested that the application be passed to issue. If the Examiner feels that a telephone conference would expedite prosecution of this case, the Examiner is invited to call the undersigned.

Respectfully submitted,

HAMILTON, BROOK, SMITH & REYNOLDS, P.C.

By 
Keith J. Wood
Registration No. 45,235
Telephone: (978) 341-0036
Facsimile: (978) 341-0136

Concord, MA 01742-9133

Dated: 5/19/06